DATE(S) ISSUED:
4/14/2010

SUBJECT:
Vulnerability in Windows Media Player 9 Could Allow Remote Code Execution (MS10-027)

OVERVIEW:
A vulnerability has been discovered in the ActiveX control for Microsoft Windows Media Player 9 which is utilized when accessing online media content such as music or a video. Microsoft Windows Media Player 9 is installed on all versions of Windows XP & 2000 by default. When vulnerabilities are discovered in the ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

> Windows XP
> Windows 2000

RISK:

Government:
> Large and medium government entities: **High**
> Small government entities: **High**

Businesses:
> Large and medium business entities: **High**
> Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Microsoft Windows Media Player 9 ActiveX control which is utilized when accessing online media content. This control provides support for a multitude of media formats and is installed on all versions of Windows XP & 2000 by default. However, this vulnerability only applies to version 9 installed on the listed Operating Systems. This vulnerability may be exploited if a user visits a maliciously crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The vulnerable ActiveX control can be disabled in Internet Explorer by setting the kill bit for the following Class Identifiers (CLSIDs):
{6BF52A52-394A-11d3-B153-00C04F79FAA6}

Further instructions on how to set the kill bit can be found at the following location:
http://support.microsoft.com/kb/240797

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Set the kill bit on the aforementioned Class Identifiers (CLSID).
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS10-027.mspx
http://support.microsoft.com/kb/240797
http://support.microsoft.com/kb/979402

Secunia:
http://secunia.com/advisories/35683/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0268

SANS:
http://isc.incidents.org/diary.html?storyid=8626